

AO 106 (Rev. 04/10) Application for a Search Warrant (Page 1)

UNITED STATES DISTRICT COURT
FOR THE
SOUTHERN DISTRICT OF OHIO

FILED
RICHARD W. NAGEL
CLERK OF COURT

2019 FEB -1 PM 1:45

U.S. DISTRICT COURT
SOUTHERN DIST. OHIO
WESTERN DIV. DAYTON

Case No. **3:19mj051**

In the Matter of the Search of)
(Briefly describe the property to be searched)
(or identify the person by name and address))
a. APPLE I PHONE 6, MODEL A1586,)
IMEI 356147092942886 (Silver iPhone in black)
case with cracked screen).)
b. APPLE I PHONE 6, MODEL A1586,)
IMEI 356147092978302 (Silver iPhone in blue)
case).)
c. SAMSUNG, Model: SM-S327VCB, Serial)
Number: 355744096352095 (Black Cell Phone)
with cracked screen).)
d. APPLE I PHONE 8S, Rose Gold iPhone)
with cracked screen in a red case.)
e. Cricket LG, Black, IMEI:)
354376094707722, S/N: 808CYEA470772)
CURRENTLY LOCATED AT US SECRET)
SERVICE, 200 WEST SECOND ST., SUITE)
#811, DAYTON, OH 45402)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:
(identify the person or describe the property to be searched and its given location):

See Attachment A.

located in the Southern District of Ohio, there is now concealed
(identify the person or describe the property to be seized):

See Attachment B.

AO 106 (Rev. 04/10) Application for a Search Warrant (Page 2)

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

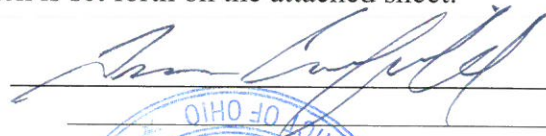
Code Section	Offense Description
18 U.S.C. 1028	Identity Theft
18 U.S.C. 1028A	Aggravated Identity Theft
18 U.S.C. 1029	Access Device Fraud
18 U.S.C. 1344	Bank Fraud
18 U.S.C. 371	Conspiracy against the United States to commit the above listed crimes

The application is based on these facts:

See Attachment.

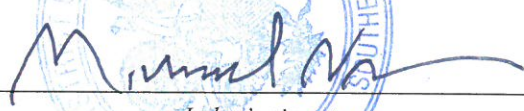
- ☒ Continued on the attached sheet.
☒ Delayed notice of 30 days (give exact ending date if more than 30 days): 3/3/19

is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


 Trevor Canfield, U.S. Secret Service
Printed name and title

Sworn to before me and signed in my presence.

Date: February 1, 2019


Judge's signature
 Hon. Michael J. Newman, U.S. Magistrate Judge
Printed name and title

City and State: Dayton, Ohio

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF

- a. APPLE I PHONE 6, MODEL A1586,
IMEI 356147092942886 (Silver iPhone in
black case with cracked screen).
- b. APPLE I PHONE 6, MODEL A1586,
IMEI 356147092978302 (Silver iPhone in blue
case).
- c. SAMSUNG, Model: SM-S327VCB,
Serial Number: 355744096352095 (Black Cell
Phone with cracked screen).
- d. APPLE I PHONE 8S, Rose Gold iPhone
with cracked screen in a red case.
- e. Cricket LG, Black, IMEI:
354376094707722, S/N: 808CYEA470772

CURRENTLY LOCATED AT US SECRET
SERVICE, 200 WEST SECOND ST., SUITE
#811, DAYTON, OH 45402

3:19mj051
Case No. _____

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, **Trevor Canfield**, Special Agent of the U.S. Secret Service, United States Department
of Justice, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal
Rules of Criminal Procedure for a search warrant authorizing the examination of property—five

electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the United States Secret Service, and have been since September 2017. I have received extensive training in conducting criminal investigations involving violations of Title 18 of the United States Code and other provisions. I am currently assigned to the Dayton Resident Office and have been trained to investigate a wide variety of financial-crime investigations, to include: Credit/Debit Card Fraud, Identity Theft, Aggravated Identity Theft, Access Device Fraud, Fraud in Connection with Computers, Bank Fraud, Wire Fraud, and Conspiracy, in violation of Title 18, United States Code, Sections 1028, 1028A, 1029, 1030, 1343, 1344, 371, and 1349 respectively. I have attended and completed multiple Law Enforcement training academies to include; The Department of Criminal Justice Training Academy (DOCJT) located in Richmond, KY, The Federal Law Enforcement Training Center (FLETC) located in Glynco, Georgia, and The United States Secret Service James J. Rowley Training Center (JJRTC) located in Laurel, Maryland. Prior to becoming a Special Agent for the United States Secret Service, I was a Patrol Deputy and a member of the Special Weapons and Tactics (SWAT) team for the Boone County Sheriff's Office located in Burlington, KY.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PURPOSE OF THE AFFIDAVIT

4. Your Affiant makes this affidavit in support of applications for search warrants for the below listed devices, as there is probable cause to believe that evidence of a crime,

contraband, or fruits of a crime, and property designed for use, intended for use, or used in committing a crime—namely, violations of 18 U.S.C. § 1028 (identity theft); 18 U.S.C. § 1028A (aggravated identity theft); 18 U.S.C. 1029 (access device fraud); 18 U.S.C. 1344 (bank fraud); and 18 U.S.C. § 371 (conspiracy of the above listed crimes) – exists and can be found on the following devices:

- a. APPLE I PHONE 6, MODEL A1586, IMEI 356147092942886 (Silver iPhone in black case with cracked screen), hereinafter “Device #1,”
 - b. APPLE I PHONE 6, MODEL A1586, IMEI 356147092978302 (Silver iPhone in blue case), hereinafter “Device #2,”
 - c. SAMSUNG, Model: SM-S327VCB, Serial Number: 355744096352095 (Black Cell Phone with cracked screen), hereinafter “Device #3,”
 - d. APPLE I PHONE 8S, Rose Gold iPhone with cracked screen in a red case, hereinafter “Device #4,” and
 - e. Cricket LG, Black, IMEI: 354376094707722, S/N: 808CYEA470772, hereinafter “Device #5;”
- (collectively referred to as “Devices”).

5. The Devices are currently located at the U.S. Secret Service, 200 West Second St. Ste. 811, Dayton, OH 45402.

6. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. The U.S. Secret Service is investigating an organized check cashing ring. On November 13, 2018, Springfield, Ohio Police Officers responded to a call from Huntington Bank, 5 W North St, Springfield, OH 45504. Bank manager Danielle Sharpe relayed that a female driving a black Jaguar, later identified as Cassandra Robidoux, attempted to pass a stolen check. Sharpe stated that Robidoux pulled up in the drive thru lane and placed in the intake tube a check written out for \$1,800, an Ohio driver's license, and a Mastercard debit card. The check belonged to Amanda Stizel and the driver's license and Mastercard debit card belonged to Kimberly Wallace. Stizel had reported that her purse containing her checkbook was stolen from her vehicle on November 12, 2018 to the Huber Heights Police Department. Kimberly Wallace had reported that her purse containing her driver's license and debit card had been stolen from her vehicle on November 10, 2018 to the Dublen Police Department.

8. Sharpe stated that Kimberly Wallace's identity had been used at different bank locations to cash \$1,800. While Robidoux was in the drive thru lane, Sharpe called Kimberly Wallace. Kimberly Wallace advised Sharpe that she was not in the drive thru lane and that her purse had been stolen. Sharpe called the police and tried to stall Robidoux but she drove off.

9. Police Officers stopped Cassandra Robidoux, driving a rented 2018 black Jaguar, near the intersection of Route 40 and Highway 68. Ohio Tag HHB4945 had been taped over Florida tag JLFU20. The vehicle also had aftermarket window tint that Avis had not installed.

10. On November 15, 2018, law enforcement interviewed Cassandra Robdioux. Robdioux was advised of her *Miranda* rights which she waived. Robdioux relayed that she is a

“runner” for an organized criminal check cashing ring headed by “Makooy.” Robdioux believes “Makooy’s” real name is Derrick. Robdioux stated there are four other black males involved, including “Reese” and “Wally.” These men go to parking lots, look for cars with women’s purses inside, and bust the vehicle’s window with a silent window punch to obtain the purses. The men want driver’s licenses and banking information from the purses. Once they obtain enough identification documents, the organization recruit women with drug addictions to portray the victims and to cash checks at matching banking establishment. These women are provided drugs to prevent them from becoming “dope sick” and ten percent of the amount written on the checks cashed.

11. Robdioux further relayed that “Makooy” instructs the recruited female drug addicts how to carry out the scheme. Specifically, “Makooy” tells the women which specific banks to go to and the amount to write on the check. He further admonishes the women to use the furthest drive thru lane from the bank teller and to stay behind the vehicle’s window tint. “Makooy” further requires the girls to keep him on speaker phone to hear what the bank teller says and to tell if the transaction is taking too long. During these transactions, “Makooy” and the other males remain in a separate vehicle at a nearby unknown location. If the transaction is successful, “Makooy” tells the woman where to meet them and then takes custody of the cash. After the stolen identifications and banking information are used, “Makooy” disposes of them.

12. According to Robidoux, the ring originated in Florida, where they rented the vehicles. They then drove to Philadelphia, then Chicago, then Ohio conducting the same scheme. The organization makes \$20,000 to \$30,000 per day they are actively working.

Robdoux identified a picture of “Makooy” as Derrick McKenzie and “Wally” as Dortelious Walken.¹

13. On November 21, 2018, the Hamilton County Sheriff’s Office Regional Narcotics Unit (RENU) Highway Interdiction Team became involved in a vehicle pursuit on I-275 westbound of a white Toyota Sienna minivan with North Carolina license plate FAP8377. The vehicle eventually came to a stop at 20 Benchway Court, Fairfield, Ohio 45014. All four occupants of the vehicle initially fled the scene but were eventually apprehended. The four occupants of the vehicle were identified as Marrice Ellis, Derrick McKenzie, Jennifer Agnew, and Kristin Blackmon. All four were arrested. The minivan was a rental vehicle registered to Advantage Rent-A-Car in the name of Marrice Ellis. A search of the vehicle recovered \$3,386.00 in cash, a stolen driver’s license belonging to S.B., marijuana, crack cocaine, a cellular phone (Device #3) found in the center console, and a vehicle rental agreement. The vehicle also had a black wig inside. Device #4 was recovered from Derrick McKenzie’s person after he was placed in custody. Device #1 and Device #2 were found on Marrice Ellis’s person after being taken into custody. Device #5 was located inside of Jennifer Agnew’s purse that was inside of the vehicle. Jennifer Agnew later turned the phone over to the Hamilton County Sheriff’s Office

¹ Derrick McKenzie was found on facebook after running his alias “Makooy” through the search bar. Facebook pictures were retrieved from the facebook profile and sent to the Cincinnati Fusion Center to try to identify the person in the photograph. The response came back identifying the subject in the photograph as Derrick McKenzie out of Ft. Lauderdale, Florida. Dortelious Walken was identified by reviewing the extraction conducted by Springfield PD of Cassandra Robidoux’s phone and locating a phone number in her contactlist under the name “Wally.” The phone number was then ran through a law enforcement database known as “The Last One” (TLO) which resulted in the identification of Dortelious Walken. A picture of Dortelious Walken was produced after running his identifying information through another law enforcement database known as the National Crime Information Center (NCIC). The picture was then shown to Cassandra Robidoux who identified the male in the picture as “Wally.”

and signed a waiver form. When interviewed by Special Agent Trevor Canfield, Agnew advised that the phone she was in possession of was bought for her by McKenzie and another.

14. On November 29, 2018, law enforcement interviewed Marrice Ellis in his hotel room at the In Town Suites Extended Stay Hotel. Ellis was advised of his *Miranda* rights and waived them. Ellis stated that Derrick McKenzie contacted him sometime between November 13 and 15, 2018 and asked Ellis to rent a car for him. McKenzie flew Ellis from Florida to Philadelphia on Spirit Airlines and instructed him to rent a vehicle at the Philadelphia airport. Ellis stated McKenzie had “picked up three prostitutes” in the Philadelphia area prior to his arrival. Ellis had “the scam all laid out,” calling it “bank fraud.” Ellis said it was his job to drive the group to Ohio to carry out the crime and knew few details other than “they were getting money from banks.” McKenzie did not tell Ellis how much money he would receive for helping but stated “ill take care of you.” When they reached Ohio, the prostitutes were put up in a Red Roof Inn and the men stayed in a separate hotel.

15. Ellis further relayed that on November 20, 2018, Ellis and the three men picked up two of the prostitutes. They were “about to go do the scame” when police attempted to stop them. Ellis relayed he attempted to flee the police because he was driving a rental vehicle. Ellis stated he was arrested “before they could do anything.” Ellis stated McKenzie “ran everything” and was the principle coordinator for the fraud they were committing.

16. On November 30, 2018, law enforcement interviewed Jennifer Agnew at the Hamilton County Justice Center. Prior to the interview, Agnew was read her *Miranda* rights and waived them. Agnew stated on November 17, 2018, a white minivan with four black males approached her on Kensington Avenue, in Philadelphia. “Mike,” identified as Derrick

McKenzie, asked if she wanted to “make some money.” McKenzie described the check cashing scheme to her and stated she would receive ten percent of each check cashed, her drug of choice, and free travel. Agnew agreed. The van traveled to a Cricket store at Kensington/Allegheny Avenue in Philadelphia. “Wally” (identified as Dortelius Walken) and McKenzie went into the store and returned with a new phone and another white female (Kristin Blackmon). McKenzie gave her the telephone. The group subsequently purchased drugs and picked up another white female Kerrie-Ann Reibo a.k.a. Kay. then purchased drugs. They drove to Ohio arriving on November 18, 2018 at a Red Roof Inn. McKenzie told Agnew to get a room and Wally provided her money. On November 19, 2018, McKenzie told Agnew to be ready to work. McKenzie and Ellis picked her up in a van and took her to a Walgreens to purchase a brush. As she left the Walgreens, Agnew observed McKenzie and Ellis unscrewing an Ohio license plate off of a truck. McKenzie and Ellis attached the stolen Ohio license plate over the van’s license plate. The group then went to a nearby gas station. Using gloves, McKenzie pulled out three checkbooks and a two-inch stack of identification and bank cards. McKenzie wrote out the checks and taught Agnew how to hold the checks to avoid getting fingerprints on them. Agnew then went to a bank and tried to cash the checks. Ellis and McKenzie stayed on speaker telephone the entire time while Agnew attempted to cash the checks. McKenzie instructed Agnew on how to respond to the bank teller’s questions. The first two attempts at cashing checks were unsuccessful. At the first bank, the bank teller asked for the victim’s mother’s maiden name. At the second bank, the bank teller advised that the check could only be deposited and not cashed. Both times McKenzie instructed Agnew to ask for the checks back which the tellers returned.

17. The group made a third attempt to cash checks. Agnew was given a black wig, two more checks, an identification, and a bank card. This time Agnew’s attempt to obtain cash

was successful. The group continued onto other banks repeating the same pattern. Agnew also went inside a couple of the banks to cash checks while Ellis and McKenzie stayed outside in the van, speaking to her via earbuds. At the last bank of the day, the teller went to the manager with the check Agnew tried to cash. Agnew overheard the manager speaking to the victim on the telephone so she left and returned to the van. Ellis and McKenzie drove down the street and removed the license plate. McKenzie gave her \$100 to purchase a hotel room for another night. After purchasing the hotel room, McKenzie gave her \$600 and told her good job. Agnew believed she cashed between \$8,000 and \$12,000 worth of checks that day. The next morning, November 20, 2018, Ellis and McKenzie picked her and one of the other girls up at the hotel. Ten minutes later, they became involved in a police chase.

18. On December 6, 2018, Jennifer Agnew turned over a cell phone (Device #5) that was used in the scheme to the Hamilton County Sheriff's Office. While interviewing Agnew she stated that she would cooperate with law enforcement anyway that she could. Agnew turned over the cell phone to show her cooperation with law enforcement and she signed a consent form for the Hamilton County Sheriff's Office to examine the cellular telephone.

19. On November 30, 2018, law enforcement interviewed Kristin Blackmon at the Hamilton County Justice Center. Blackmon was provided her *Miranda* rights and waived them. Blackmon stated "Wally" recruited her on Kensington Avenue in Philadelphia, Pennsylvania to cash checks. McKenzie and Wally promised her anywhere from \$400 to \$1000 per day to cash checks and would provide room and board. Wally also gave Blackmon \$50 to purchase the drug of her choice, heroin. Blackmon said two other girls were recruited with her, Jennifer Agnew, and Kerrie Ann Reibo (Kay). Blackmon said the group left Philadelphia on November 18, 2018,

and traveled to the Red Roof Inn located in Blue Ash, Ohio. Agnew purchased a hotel room with money provided by McKenzie. The next day, November 19, 2018, McKenzie and Ellis only picked up Agnew. On November 20, 2018, McKenzie and Ellis picked up Agnew and Blackmon. Ellis was mad at Blackmon because she had dyed her hair blue. Ellis told Blackmon "Why would you do that when you look just like this girl? Your fucking stupid tell her to get the fuck out." While in the car, McKenzie handed Blackmon a stolen driver's license of a lady with the last name Tauney. Shortly after she received the driver's license, the van became involved in a high speed pursuit. Blackmon stated McKenzie was in charge and kept the banking and identifying information while Ellis was the driver.

20. Based on my training, experience, knowledge of this case, and discussions with fellow agents, I know that check cashing rings use telephones to communicate. The handler often communicates with the runner, the person cashing checks, during transactions. The handler is outside in a vehicle, or at an unknown location while the runner is in the drive thru lane or inside of the banking establishment speaking with the teller. The runner is instructed by the handler to keep the phone on speaker phone so that he can hear everything the bank teller is saying. The handler will tell the runner what to say to a bank teller. The runner is also instructed to wear headphones so that when the handler advises the runner on how to respond to the question or situation, only the runner can hear him. The handler also sets a timer and once the time runs out he advises the runner to leave everything and drive off or walk away. The handler advises the runner if he feels that the teller is stalling for law enforcement.

21. The Devices are currently in the lawful possession of the United States Secret Service. They came into the United States Secret Service's possession in the following way: On

November 21, 2018, RENU Agents from the Hamilton County Sheriff's Office became involved in a vehicle pursuit of a white van. Device #1 and Device #2 were recovered from Marrice Ellis's person, Device #3 was located inside of the center console of the vehicle, and Device #4 was recovered from Derrick McKenzie's person. These Devices were seized pursuant to arrest. Jennifer Agnew turned in Device #5 and signed a Hamilton County Sheriff's Office electronic consent form, therefore, Device #5 was seized by consent. Therefore, while the United States Secret Service might already have all necessary authority to search the Device, I seek this additional warrant out of an abundance of caution to be certain that a search of the Device will comply with the Fourth Amendment and other applicable laws.

22. The Devices are currently in storage at the U.S. Secret Service, 200 West Second Street Suite #811, Dayton, Ohio 45402. They previously had been stored by RENU Agents from the Hamilton County Sheriff's Office. In my training and experience, I know that the Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the United States Secret Service.

TECHNICAL TERMS

23. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of

transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
- g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a

telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

- h. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

24. Based on my training, experience, and research, I know that the Devices have capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

25. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

27. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

28. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

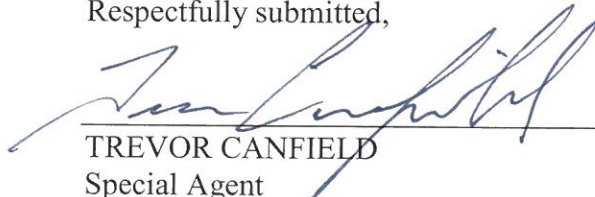
CONCLUSION

29. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

30. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,


TREVOR CANFIELD
Special Agent
U.S. Secret Service

Subscribed and sworn to before me
on February 1, 2019:


UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Error! Reference source not found.

- a. APPLE I PHONE 6, MODEL A1586, IMEI 356147092942886
- b. APPLE I PHONE 6, MODEL A1586, IMEI 356147092978302
- c. SAMSUNG, Model: SM-S327VCB, Serial Number: 355744096352095
- d. APPLE I PHONE 8S
- e. Cricket LG, IMEI: 354376094707722, S/N: 808CYEA470772

(Collectively, the “**Devices**”). This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of 18 U.S.C. § 1028 (identity theft); 18 U.S.C. § 1028A (aggravated identity theft); 18 U.S.C. 1029 (access device fraud); 18 U.S.C. 1344 (bank fraud); and 18 U.S.C. § 371 (conspiracy of the above listed crimes) and involve **DERRICK MCKENZIE, MARRICE ELLIS, JENNIFER AGNEW, KRISTIN BLACKMON** since January 1, 2018, including:

- a) records regarding the use of funds to include records of any financial accounts or financial transactions;
- b) records of communication to include emails, Facebook, letters, facsimile transmissions, notes, text, or other correspondence;
- c) Records to determine attribution of particular relevant communications or other evidence, for example any information that would help identify the creator, sender or recipient of data or communications;
- d) Evidence of who used or controlled computers or other electronic media at the time the items described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- e) Records of personal or business activities relating to the operation or ownership of any computer hardware, software, storage media, or data (such as user names, passwords, telephone records, notes, books, diaries, and reference materials);

- f) Records pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media;
- g) Passwords, encryption keys, and other access devices that may be necessary to access data or information;
- h) Information concerning internet use and searches, including, websites searched, “visited” and otherwise contacted, including search history and paths, files downloaded and saved, as well as deleted files;
- i) Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts;
- j) Location data, including GPS data.
- k) Contextual information necessary to understand the evidence described in this attachment; and
- l) Records and things evidencing the use of the Internet to communicate including:
 - i) records of Internet Protocol addresses used; and
 - ii) records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user typed web addresses.
- m) lists of customers and related identifying information; types, amounts, and prices of PII purchased or sold as well as dates, places, contents and amounts of specific transactions;

- n) Genuine Credit Card Account Numbers used.
- o) Any information related to sources of Genuine Personal Bank Checks and Credit Card Account Numbers (including names, addresses, phone numbers, or any other identifying information);
- p) Any information recording **ELLIS, MCKENZIE, AGNEW** and **BLACKMON'S** schedule and/or travel from January 1, 2018 to the present;
- q) All bank records, checks, credit card bills, account information, and other financial records;
- r) Any text messages and/or communications with others;
- s) GPS or navigation information;
- t) Information downloaded from the internet onto the cellular phone, such as email, social network information (like "Facebook"), travel information such as maps or directions, and photographs; and
- u) Call data, such as missed calls, received calls, and dialed calls.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.